

REMARKS

Reconsideration of the application is requested in view of the amendments above and comments which follow.

Claim Objections

In light of the Examiner's suggestion in paragraph 1 of the Office Action, claim 1 has been amended so that at parts (c) and (d) the word "allowing" replaced by the word "enabling". In claims 2 and 3 the word "allowing" is replaced with the word "requiring".

In light of the Examiner's suggestion at paragraph 2 of the Office Action claim 7 has been amended to read "A method of operating a computer system...".

Claim Rejections - 35 USC § 103

Applicants have considered US 6,662,228 (Limsico) and US 6,973,482 (Mohammed) in detail.

Limsico

It is respectfully submitted that the portions of Limsico that the Examiner considers relevant to claim 1 do not disclose parts (a)-(c) of the computer system of claim 1.

As explained in the first three columns of Limsico, a problem arises in relation to the secure authentication and authorizing of users over an insecure channel.

The description of remote network administration at lines 34-52 of column 3 of Limsico address two particular issues relevant to authentication and authorization of users in remotely administered networks. The first is to the desirability of providing access, authorization and authentication through encrypted means, and the second is that it is more convenient to provide an authentication and authorization database of administrators which is under control of the network administrator. The use of a

centralized authentication and authorization database allows convenient removal, replacement and addition of administrators rather than requiring updating of separate databases on remotely administered networks. As can be appreciated from the description of the embodiment of Figure 2, which forms the basis of the Examiner's objections to claims 1-3, Limsico teaches:

1. An administrator at an administrator's work station accesses a network over a remote channel;
2. An authentication server on the accessed network attempts to establish and authenticate the administrator's identity using the information in a local authentication database and authentication server;
3. If the administrator is not among the ordinary users of the remotely administered network listed in the local authorization database, the administrator's identity is not authenticated, and the authentication enquiry is moved on to the second authentication server (column 5, lines 24-44).

The "alternative" and "second alternative" embodiments described in column 6 of Limsico are systems in which the local authentication server does not expect to be able to authenticate all remote administrators *a priori*. In these embodiments the authentication is automatically passed on to the second authentication server. In the "second alternative" embodiment there are a plurality of second authentication servers each of which can authenticate the identity of a selection of administrators known to them.

Mohammed

The Examiner accepts that Mohammed is only relevant to the establishment of remote-login shadow sessions in which the computer expert is able to establish a connection with a user computer, allowing the expert to view the desktop of the user computer.

Differences between the cited art and the invention as claimed

Figure 2 of Limsico and the passages cited by the Examiner as relevant to parts (a) and (b) of claim 1 do not show a first network including a plurality of client computers and a first server computer. In the analogy made by the Examiner, the work station 202 of Limsico correspond to a client computer of (a), however the work station 202 is not connected to a server on the same network, and there are no other client computers on the same network. Correspondingly there is no teaching of and no need for log-on software to enable the user at one of the first client computers to log on to the first server computer.

The teaching of Limsico does not encompass a plurality of further networks. The client network 206 of Limsico stands alone without further networks.

The material of part (c) of claim 1 is not taught by Limsico, as there is no *inter-server* log-on between networks.

Limsico does not have any teaching relevant to running a remote desktop session, as acknowledged by the Examiner.

Problem/Advantages

The problem addressed by the present invention is set out in the paragraphs bridging pages 1-2 as originally filed. The linking of work stations for support staff directly to each customer network is inefficient.

Limsico still retains a one to one relationship between network administrator work stations and the client networks. It is clear therefore that the present invention overcomes the problem of Limsico in relation to breaking a link between individual network administrators and the remotely administered network that each administrator can access.

The view of the person of ordinary skill in the art, and obviousness

The person of ordinary skill in the art of computer systems, when faced with Limsico would be primarily concerned with the vulnerabilities introduced into the system by communication over an insecure channel.

The person of ordinary skill in the art would recognize a disadvantage with the Limsico system in relation to the use of a second authentication server external to the network 206. The second external authentication server introduces a point of weakness in the security of the authentication system. The remotely administered network will accept access requests from administrators on the basis of an authentication provided by the second authentication server, but the remotely administered network has no control over and indeed no knowledge of whether or not the security of the second authentication server has been compromised in some way.

Applicants therefore submit that it would not have been obvious to the person of ordinary skill in the art to work from Limsico when considering the problem set out in the present application, and that to the extent that the person of ordinary skill in the art takes anything from Limsico it is that it is possible to allow network administrators more convenience in updating the credentials needed for network authentication at the expense of introducing an extra security vulnerability in the system.

It would not have been obvious to modify Limsico in such a way to move toward the invention of claim 1. The invention of claim 1 does not operate as if a combination of known methods, and goes beyond the predictable results expected from a combination of the cited art.

The above arguments apply equally to claim 7.

Considering claim 2, the portion of Limsico at column 6, line 32-43 cited by the Examiner does not teach the presentation by the first server computer of a list of further networks that a user is permitted to access.

In Limsico there is only a single remotely administered network 206, with a number of further authentication servers provided outside of the first network and the

remotely administered network to provide external authentication to different users based on the user's identification. Claim 2 therefore would not have been obvious in light of Limsico.

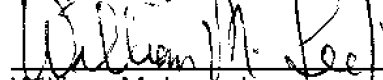
The remaining dependent claims submitted to be allowable at least by virtue of their dependency on the allowable claim 1.

It is therefore submitted that the application, as amended, is now in condition for allowance, and the Examiner's further and favorable reconsideration in that regard is urged.

As this Response is being sent during the fifth month following the Examiner's Office Action, an appropriate Petition for Extension of Time is also submitted herewith.

August 7, 2007

Respectfully submitted,



William M. Lee, Jr.

Registration No. 26,935

Barnes & Thornburg

P.O. Box 2786

Chicago, Illinois 60690-2786

(312) 214-4800

(312) 759-5646 (fax)